UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against- Case No. 12 Cr. 185 (LAP)

JEREMY HAMMOND,

Defendant.

EXHIBIT H ADDITIONAL RELEVANT CONDUCT

LAW OFFICES OF SUSAN G. KELLMAN
25 EIGHTH AVENUE • BROOKLYN, NEW YORK 11217
(718) 783-8200 • FAX (718) 783-8226 • KELLMANESQ@AOL.COM
FELLOW, AMERICAN COLLEGE OF TRIAL LAWYERS

November 1, 2013

The Honorable Loretta A. Preska
Chief Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: United States v. Jeremy Hammond
12 Cr. 185 (LAP)

Dear Judge Preska

Please accept this letter as an addendum to our sentencing submission on behalf of Mr. Jeremy Hammond.

We have devoted a large portion of our main submission to Mr. Hammond's motivations and other relevant Section 3553(a) factors. In the course of reviewing the discovery in this case, it has become clear that the Stratfor hack and the relevant conduct to which Mr. Hammond pled guilty are only part of the story, and that there are additional hacks and conduct by Mr. Hammond that are appropriate for the Court's consideration under 18 U.S.C. § 3553(a) as they are part of the nature and circumstances of the offense and they provide the contextual framework for the Court's overall consideration of Mr. Hammond's intentions and motivation.[1]

Following the Stratfor hack, Mr. Hammond, through the government's agent Hector Monsegur, aka "Sabu," was asked to hack a number of websites and computer servers outside of the United States. Mr. Monsegur supplied lists of targets, which included numerous foreign government websites and affected over 1000 domains.[2]

---

[1] Since much of the substance contained in this submission is arguably within the limitations set by the Protective Order in place, in an excess of caution, we are filing a redacted version on ECF, but will provide Chambers and government counsel with this unredacted submission.

[2] Many of these target websites utilized the popular Plesk web-hosting software and were subject to a hidden vulnerability, which only Jeremy Hammond a few others had the tools to access. This vulnerability permitted attackers to access and control the servers remotely.

For example, on January 23, 2012, Mr. Monsegur gave Mr. Hammond a list of [redacted] government targets to "hit…for our [redacted] squad." Mr. Hammond hacked one of the targets and showed Monsegur that it contained 287 domains and 1330 different email accounts. Monsegur told Hammond that "havitja…our boy thats been dosing and hacking [redacted] past few days gonna handle it.[3]"

Upon information and belief, access to the sites was then passed on to Havittaja, who used the information to target the [redacted] government and its institutions.[4] After Mr. Monsegur was publicly revealed as a government cooperator, a person who was identified as the [redacted] hacker Havittaja published what he/she claimed was a portion of his/her chat room correspondence with Monsegur on the internet.[5] The question Havittaja asked is "why was he giving me passwords if he was with the FBI?"

Mr. Hammond accepts full responsibility for his unlawful conduct, and nothing in this letter is intended to minimize or detract from his responsibility for the actions that he took. Nonetheless, the question raised by Havittaja is a valid one. Why was our government, which presumably controlled Mr. Monsegur during this period, using Jeremy Hammond to collect information regarding the vulnerabilities of foreign government websites and in some cases, disabling them? This question is especially relevant today, amidst near daily public revelations about governments' efforts, worldwide, to monitor the communications of, and gather intelligence on, world leaders.

The discovery in this case, further reveals that while cooperating with the government, Mr. Monsegur challenged Mr. Hammond to access many international government websites and servers, including sites associated with [redacted] Significantly, the [redacted] targets included the [redacted] and the [redacted] targets included the television giant [redacted]

Over the course of numerous chat logs, Mr. Monsegur, presumably under

---

[3] The online pseudonym of this hacker is actually "Havittaja."

[4] [redacted]

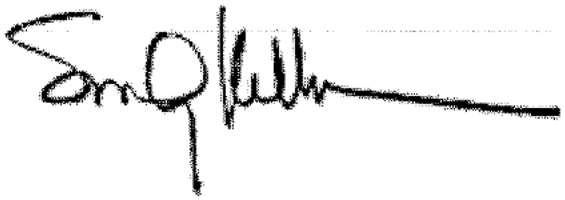
[5] See http://pastebin.com/pqimeV3n, attached as Exhibit 2

government direction, repeatedly asked Mr. Hammond to provide passwords or root backdoor information to access these sites. In some cases, as with at least some of the [redacted] targets, which were passed on to Havittaja, and some of the [redacted] targets, which appear to have been passed on to a [redacted] hacking group known as "Red Hack," it appears as though the United States government was actively facilitating the hacking of foreign government websites. In other cases, Mr. Hammond provided site access information to Mr. Monsegur, but it is unclear if any action was taken, or what, if any, intelligence information was collected by the United States. It is possible that some of these vulnerabilities mined by Mr. Hammond, at Mr. Monsegur's direction, still exist, and that the government possesses the means to access these sites.

We have attached, for the Court's review, a summary of the discovery materials that relate to this activity, as well as the bate stamped pages of discovery that corresponds to this summary.

Thank you for your kind consideration of these materials.

Respectfully submitted,



Susan G. Kellman
Sarah Kunstler
Attorneys for Jeremy Hammond
25 Eighth Avenue
Brooklyn, New York 11217
(718) 783-8200
kellmanesq@aol.com

cc: AUSA Rosemary Nidiry
AUSA Thomas Brown
Susan P. Matthews, USPO

Jeremy Hammond

DISCOVERY TIMELINE PERTAINING TO HACKS OF FOREIGN WEBSITES

01/23/12

- Mr. Monsegur gives Mr. Hammond a list of [redacted] targets with Plesk vulnerabilties[1] and asks him to "hit these....for ou[redacted]squad." (BS 104988 – 104989)
- Hammond hacks one of these targets and shows Monsegur the site contains 287 domains and 1330 different email accounts. Monsegur says he will give these targets to [redacted]hacker "Hivitja" (actually Havittaja) to hack the sites. Monsegur tells Hammond to create a root backdoor ("just backdoor urls") so the sites can be accessed again. Hammond also gives Monsegur passwords for some of the sites. [2] (BS 104989 – 104990)
- Monsegur identifies additional targets for Hammond. Hammond confirms that he successfully gained access to two of them. One of the servers contains 3520 domains, many of them in [redacted] and [redacted] Another contains 392 [redacted] domains. (BS 104991-105013)
- Hammond explains to Monsegur how to use root backdoors and where to find the email and databases. (BS 105013-105014)
- Monsegur says he is finding more targets ("finding new juicy targets") and asks for root backdoor instructions again, which Hammond provides. (BS 105014)
- Monsegur provides Hammond with targets in [redacted] Hammond gains access to one that contains 62 domains and 96 email accounts. (BS 105028-105029)
- Monsegur provides more international targets, says he is "looking for embassys [sic] and consulates" [sic]. Hammond provides access to two of them. (BS 105029-105030)
- Monsegur asks Hammond to access a [redacted] site, but he is unable to gain access. (BS 105041)
- Monsegur gives Hammond more [redacted] targets, including [redacted] which he describes as a "big target." Hammond provides passwords. (BS 105041-105042)
- Monsegur provides more [redacted] targets. Hammond gains access to one of them and provides the password, as requested. (BS 105044-105046)

---

1 In the discovery, Plesk vulnerabilities are indicated with the [redacted] a vulnerable port on Plesk websites.

2 For sites that ran on Linux, Mr. Hammond was able to provide backdoors. For Windows-based sites, he was only able to provide passwords for administrative access.

3 [redacted] s a [redacted] media conglomerate and the [redacted]

1/25/12

- Monsegur provides a long list of targets from many different international countries including [redacted] (BS 105061-105063)
- Monsegur tells Hammond that he will give the [redacted] government sites to a [redacted] hacking group known as RedHack ("the [redacted] will be handled RedHack famous [redacted] hackers") and tells Hammond that the sites he has given him are "high priority" -- as if he were placing an order. (BS 105063)
- Monsegur invites Hammond to the RedHack channel so Hammond can provide the [redacted] sites ("accept invite"). Monsegur also provides more [redacted] domains (BS 105065-105066)
- Hammond tells Monsegur that one of the servers has mail for 22 [redacted] government domains and another has mail for about 600 domains. (BS 105067.)
- Monsegur creates a chat room and invites Hammond and an alleged member of RedHack. They exchange information regarding thousands of [redacted] sites. (BS 62889)
- Hammond explains to the alleged Redhack member how to access the root backdoors of the [redacted] sites. (BS 62889-62897)

1/26/12

- Monsegur follows up on foreign government targets he provided to Hammond "last night." Hammond sends back a list of the sites he did not gain access to, including government sites in [redacted] (BS 105077-105078)
- Monsegur asks for the list again. Monsegur again asks for instructions on how to access root backdoors. Hammond gives Monsegur the information (BS 105080-105081)
- Monsegur provides two [redacted] government targets and asks Hammond to provide passwords. (BS 105088)
- Monsegur provides more [redacted] targets to which he wants access. (Monsegur: "lend me an hour of your time to bang out these [redacted] targets.") Hammond gains access to one that hosts 7 domains and 56 email accounts. (BS 105091)
- Monsegur provides two targets in [redacted] Hammond cannot gain access to either. (BS

105091-105092)

2/2/12

- Monsegur provides more targets, including a government site in [redacted] and government sites in [redacted] Mr. Monsegur asks again for instructions on how to access root backdoors. (BS 105152)

- Monsegur provides targets in [redacted] Hammond acceses one of the [redacted] sites that contains 135 domains and 287 email accounts (BS 105157-105159)

2/15/12

- Monsegur provides targets in [redacted] He tells Hammond that these sites are for "tony, the guy who hacked kingcope" (BS 67593-67594)

- Monsegur tells Hammond he is "setting up a new box to serve as another tor onion for us as a third backup" and says "I want us to have redundant backups for all our shit." (BS 67594-67595)

- Hammond provides access to some of the [redacted] sites. He creates three backdoors and tells Monsegur that they contain hundreds of domains and emails. Hammond comments "hopefulyl were getitngs omething out of all this" and Monsegur responds "trust me…everything i do serves a purpose ;P" (BS 67597)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against- Case No. 12 Cr. 185 (LAP)

JEREMY HAMMOND,

Defendant.

EXHIBIT H

EXHIBIT 1 – NEWS REPORT ON [redacted] HACKS

REDACTED

REDACTED

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against- Case No. 12 Cr. 185 (LAP)

JEREMY HAMMOND,

Defendant.

EXHIBIT H

EXHIBIT 2 – ALLEGED STATEMENT BY HAVITTAJA

24/01/2012
https://twitter.com/Havittaja
https://twitter.com/theevilc0de
One of the last conversations with Sabu.
WHAT REALLY SABU WAS DOING.

A QUESTÃO É porque ele estava me dando senhas se ele estava com o FBI?
THE QUESTION IS why he was giving me passwords if he was with the FBI?

censored password obvious reasons

18:51 Havittaja hey
18:51 Sabu my brother!!!
18:51 Havittaja what's happen
18:52 Havittaja ;D
18:52 Sabu FTP:
18:52 Sabu [redacted]censored
18:52 Sabu [redacted] censored
18:52 Sabu root:
18:52 Sabu http://censored/[redacted]
18:52 Sabu [redacted]for root
18:52 Sabu [redacted]
18:52 Sabu [redacted]for admin password
18:52 Havittaja ohh
18:52 Havittaja its for me ?
18:53 Sabu I showed lala/hard366 as well but I don't think they'll do something with the root
18:53 Sabu also
18:53 Sabu for the first 2, they're on the same server with hundreds of [redacted] domains
18:53 Sabu you have control of them. I can give you the xml file with all passwords
18:53 Sabu want them?
18:53 Havittaja hm sure
18:54 Havittaja so i'll wait evilc0de
18:54 Havittaja we working together
18:54 Sabu ok
18:54 Sabu the most important is the [redacted]
18:55 Havittaja oky

ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored
ftp:[redacted]user: censored pass: censored

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against- Case No. 12 Cr. 185 (LAP)

JEREMY HAMMOND,

Defendant.

EXHIBIT H

EXHIBIT 3 – CITED CHATS

Conversation with yohoho@jabber.ccc.de at 2/15/2012 4:44:14 PM on LeonDavidson@jabber.org/jabber.org (jabber)

(4:44:19 PM) **leondavidson@jabber.org/jabber.org:** what up broham
(4:44:32 PM) **yohoho@jabber.ccc.de:** yoyo
(4:44:40 PM) **yohoho@jabber.ccc.de:** hackin and crackin u???
(4:45:14 PM) **leondavidson@jabber.org/jabber.org:** about to take a nap
(4:45:20 PM) **yohoho@jabber.ccc.de:** nice, nice
(4:45:41 PM) **leondavidson@jabber.org/jabber.org:** my schedule is fucked plus works beating my ass
(4:45:54 PM) **leondavidson@jabber.org/jabber.org:** I missed th[redacted] defacement the other night ya nig!
(4:46:38 PM) **leondavidson@jabber.org/jabber.org:** couple of things:
(4:46:39 PM) **yohoho@jabber.ccc.de:** yeah
(4:46:40 PM) **yohoho@jabber.ccc.de:** well
(4:46:43 PM) **yohoho@jabber.ccc.de:** I had to hit it hard
(4:46:46 PM) **yohoho@jabber.ccc.de:** admins started removing backdoors
(4:46:59 PM) **yohoho@jabber.ccc.de:** they removed my password loggers and shit
(4:47:02 PM) **yohoho@jabber.ccc.de:** so I had to go fast
(4:47:10 PM) **leondavidson@jabber.org/jabber.org:** mhm
(4:47:15 PM) **leondavidson@jabber.org/jabber.org:** tats what elche told me
(4:47:17 PM) **leondavidson@jabber.org/jabber.org:** thats whats up
(4:47:20 PM) **leondavidson@jabber.org/jabber.org:** it worked out actually
(4:47:28 PM) **yohoho@jabber.ccc.de:** good thing it ended up being timed great
(4:47:33 PM) **leondavidson@jabber.org/jabber.org:** I guess shit happens for a reason. that box was just too full of holes
(4:47:39 PM) **leondavidson@jabber.org/jabber.org:** fucking fckeditor hole is a joke
(4:47:43 PM) **leondavidson@jabber.org/jabber.org:** for a company like[redacted]
(4:47:44 PM) **yohoho@jabber.ccc.de:** for real
(4:47:52 PM) **yohoho@jabber.ccc.de:** that's how becca's other sites got hacked too
(4:47:57 PM) **yohoho@jabber.ccc.de:** according to the last email on that defacement
(4:48:00 PM) **leondavidson@jabber.org/jabber.org:** mhm
(4:48:11 PM) **yohoho@jabber.ccc.de:** she just got fired from her other job
(4:48:24 PM) **leondavidson@jabber.org/jabber.org:** that sucks
(4:48:25 PM) **yohoho@jabber.ccc.de:** I still have one of her email addresses
(4:48:27 PM) **leondavidson@jabber.org/jabber.org:** aha feel bad for her
(4:48:33 PM) **yohoho@jabber.ccc.de:** well
(4:48:37 PM) **yohoho@jabber.ccc.de:** she obviously knew who[redacted]was
(4:48:41 PM) **leondavidson@jabber.org/jabber.org:** jea
(4:48:44 PM) **yohoho@jabber.ccc.de:** because in her emails she showed hesitation
(4:48:46 PM) **yohoho@jabber.ccc.de:** about working fo rhtem
(4:48:49 PM) **yohoho@jabber.ccc.de:** but she did it anyway
(4:49:24 PM) **yohoho@jabber.ccc.de:** she's honestly lucky we didn't post both of her mail spools
(4:49:28 PM) **yohoho@jabber.ccc.de:** she has dating profiles and everything
(4:49:32 PM) **yohoho@jabber.ccc.de:** eharmony, plentyoffish
(4:49:39 PM) **leondavidson@jabber.org/jabber.org:** she hot?

(4:49:48 PM) **yohoho@jabber.ccc.de:** I didn't look at her profile actually
(4:49:53 PM) **leondavidson@jabber.org/jabber.org:** haha
(4:49:55 PM) **yohoho@jabber.ccc.de:** you dirty bastard =p
(4:49:58 PM) **leondavidson@jabber.org/jabber.org:** yo a few things brother
(4:50:00 PM) **leondavidson@jabber.org/jabber.org:** first
(4:50:09 PM) **leondavidson@jabber.org/jabber.org:** h's boy has plesk bug as you know
(4:50:12 PM) **leondavidson@jabber.org/jabber.org:** so he messages me with:
(4:50:19 PM) **leondavidson@jabber.org/jabber.org:** 5:48 <bf1> yo
15:48 <bf1> you around?
15:48 <bf1> [redacted]is vuln
15:48 <bf1> its running plesk
15:49 <bf1> i just found it during a search
15:49 <bf1> ;)

(4:50:22 PM) **yohoho@jabber.ccc.de:** h's boy ?
(4:50:24 PM) **leondavidson@jabber.org/jabber.org:** so makes sense we tell him to leave it alone
(4:50:28 PM) **leondavidson@jabber.org/jabber.org:** yes. bf/bf1
(4:50:30 PM) **yohoho@jabber.ccc.de:** fuck
(4:50:32 PM) **leondavidson@jabber.org/jabber.org:** thats h's boy
(4:50:34 PM) **yohoho@jabber.ccc.de:** we already have that box
(4:50:40 PM) **yohoho@jabber.ccc.de:** damnit
(4:50:43 PM) **yohoho@jabber.ccc.de:** maybe we should hit it on friday
(4:50:48 PM) **leondavidson@jabber.org/jabber.org:** I'll tell him to leave it alone. but you never know ...
(4:50:49 PM) **leondavidson@jabber.org/jabber.org:** its tainted
(4:50:53 PM) **leondavidson@jabber.org/jabber.org:** fee me
(4:50:55 PM) **leondavidson@jabber.org/jabber.org:** feel*
(4:50:56 PM) **yohoho@jabber.ccc.de:** let's hit it on friday
(4:50:59 PM) **leondavidson@jabber.org/jabber.org:** kk
(4:51:00 PM) **leondavidson@jabber.org/jabber.org:** another thing
(4:51:05 PM) **leondavidson@jabber.org/jabber.org:** had a very long talk with kingcope
(4:51:06 PM) **yohoho@jabber.ccc.de:** we need a FFF from now on
(4:51:09 PM) **yohoho@jabber.ccc.de:** yes?
(4:51:11 PM) **leondavidson@jabber.org/jabber.org:** he sends his love to our team
(4:51:14 PM) **leondavidson@jabber.org/jabber.org:** he says thank you
(4:51:19 PM) **yohoho@jabber.ccc.de:** that is awesome
(4:51:20 PM) **leondavidson@jabber.org/jabber.org:** that "we need this to happen"
(4:51:24 PM) **leondavidson@jabber.org/jabber.org:** and
(4:51:32 PM) **leondavidson@jabber.org/jabber.org:** he's sending us research asap that is not paid for
(4:51:37 PM) **leondavidson@jabber.org/jabber.org:** sadly his remote mysql 0day = paid work
(4:51:42 PM) **leondavidson@jabber.org/jabber.org:** he cant send it to us out of respect
(4:51:46 PM) **leondavidson@jabber.org/jabber.org:** but he has other shit
(4:52:38 PM) **leondavidson@jabber.org/jabber.org:** got a few requests from [redacted]proters. give me a minute
(4:53:16 PM) **leondavidson@jabber.org/jabber.org:** another thing

(4:53:26 PM) **leondavidson@jabber.org/jabber.org:** LoD send us complete source codes for norton anti-virus:
(4:53:28 PM) **leondavidson@jabber.org/jabber.org:** 20:39 <LoD> [redacted]
20:39 <LoD> [redacted]
20:39 <LoD>
20:39 <LoD>
20:39 <LoD>
20:39 <LoD>
(4:53:43 PM) **yohoho@jabber.ccc.de:** oh wow
(4:53:47 PM) **yohoho@jabber.ccc.de:** what are we going to do about that ?
(4:53:56 PM) **leondavidson@jabber.org/jabber.org:** they asked me to promsie we doont release it
(4:53:58 PM) **yohoho@jabber.ccc.de:** I understand about the mysql shit
(4:53:59 PM) **leondavidson@jabber.org/jabber.org:** but to use it for our research
(4:54:03 PM) **yohoho@jabber.ccc.de:** ok so what are we going to do, audit it?
(4:54:07 PM) **leondavidson@jabber.org/jabber.org:** malware research
(4:54:08 PM) **leondavidson@jabber.org/jabber.org:** yup
(4:54:18 PM) **yohoho@jabber.ccc.de:** we might need someone who ahs a lot of time and experience with this
(4:54:22 PM) **yohoho@jabber.ccc.de:** im not the right person
(4:54:33 PM) **yohoho@jabber.ccc.de:** and also I'm putting alex to work on some shit as well
(4:54:52 PM) **yohoho@jabber.ccc.de:** oh ok wait
(4:54:52 PM) **yohoho@jabber.ccc.de:** bf
(4:54:55 PM) **leondavidson@jabber.org/jabber.org:** thats fine. I'm just sendning you the data to have just in case
(4:54:55 PM) **yohoho@jabber.ccc.de:** is blowfish ?
(4:54:56 PM) **yohoho@jabber.ccc.de:** foof ?
(4:55:00 PM) **leondavidson@jabber.org/jabber.org:** nein
(4:55:10 PM) **leondavidson@jabber.org/jabber.org:** hes the kid that sent us all thse .mil.,gov logins
(4:55:11 PM) **yohoho@jabber.ccc.de:** hmm ok because blowfish works with revolusec and knwos about plesk but he doesn't have the sploit
(4:55:16 PM) **yohoho@jabber.ccc.de:** oh right
(4:57:15 PM) **leondavidson@jabber.org/jabber.org:** [redacted]
(4:57:27 PM) **yohoho@jabber.ccc.de:** ok let me take a look
(4:57:37 PM) **leondavidson@jabber.org/jabber.org:** [redacted]
(4:57:40 PM) **yohoho@jabber.ccc.de:** also
(4:57:43 PM) **leondavidson@jabber.org/jabber.org:** this is for tony, the guy that hacked

kingcope
(4:57:54 PM) **yohoho@jabber.ccc.de:** I owned the fuck out of some [redacted] domains, some [redacted] domains, and Imay have insane leads on dozens of [redacted] boxes
(4:57:57 PM) **yohoho@jabber.ccc.de:** thousands of [redacted] domains
(4:58:05 PM) **yohoho@jabber.ccc.de:** I am already talking to someone from [redacted] who runs #op[redacted]
(4:58:14 PM) **leondavidson@jabber.org/jabber.org:** awesome
(5:02:23 PM) **yohoho@jabber.ccc.de:** yes I will try to make preparations for thursday night
(5:02:26 PM) **yohoho@jabber.ccc.de:** maybe early as hell friday morning
(5:02:28 PM) **yohoho@jabber.ccc.de:** on this [redacted] target
(5:02:29 PM) **yohoho@jabber.ccc.de:** ok?
(5:03:40 PM) **leondavidson@jabber.org/jabber.org:** ja
(5:05:32 PM) **leondavidson@jabber.org/jabber.org:** any word on those [redacted] targets?
(5:05:59 PM) **yohoho@jabber.ccc.de:** give me 10
(5:06:03 PM) **yohoho@jabber.ccc.de:** eating
(5:06:16 PM) **leondavidson@jabber.org/jabber.org:** ja for sure
(5:06:18 PM) **leondavidson@jabber.org/jabber.org:** talkign to tony
(5:06:20 PM) **leondavidson@jabber.org/jabber.org:** I love this nigga
(5:06:37 PM) **leondavidson@jabber.org/jabber.org:** he has a spy within kingcope's circle
(5:06:44 PM) **leondavidson@jabber.org/jabber.org:** and kcope was bragging he spoke to me this morning
(5:06:54 PM) **leondavidson@jabber.org/jabber.org:** so tony's like. dont ttrust him. just fuck him more
(5:07:05 PM) **leondavidson@jabber.org/jabber.org:** (I think tonys going to own [redacted] again)
(5:07:05 PM) **leondavidson@jabber.org/jabber.org:** haha
(5:07:21 PM) **leondavidson@jabber.org/jabber.org:** anyway enjoy your food. hit me up when you're done
(5:15:56 PM) **yohoho@jabber.ccc.de:** ok back
(5:15:59 PM) **yohoho@jabber.ccc.de:** also talking to value
(5:16:05 PM) **yohoho@jabber.ccc.de:** about maybe ddosin' some sites on friday as well
(5:16:09 PM) **yohoho@jabber.ccc.de:** so we have deface and ddos line dup
(5:16:17 PM) **leondavidson@jabber.org/jabber.org:** yup
(5:16:27 PM) **leondavidson@jabber.org/jabber.org:** his net is growing. he has some new malware spreading here and there
(5:16:46 PM) **yohoho@jabber.ccc.de:** he is really interested in [redacted] targets
(5:16:49 PM) **yohoho@jabber.ccc.de:** but I dont' know what to tell him
(5:16:54 PM) **yohoho@jabber.ccc.de:** it's not my call, I can't give him anything
(5:17:34 PM) **leondavidson@jabber.org/jabber.org:** yeah hes been asking me for it etc. I said I try what I can do [redacted] so [redacted] has ties to [redacted] etc. he wants to help the sauce against [redacted] etc
(5:17:42 PM) **leondavidson@jabber.org/jabber.org:** niggas be passionate about all this ish
(5:18:12 PM) **leondavidson@jabber.org/jabber.org:** setting a new box to serve as another tor onion for us as a third backup
(5:18:18 PM) **leondavidson@jabber.org/jabber.org:** ill give you details soon
(5:18:28 PM) **leondavidson@jabber.org/jabber.org:** I want us to have redundant backups for all

our shit
(5:18:33 PM) **yohoho@jabber.ccc.de:** I agree
(5:19:15 PM) **leondavidson@jabber.org/jabber.org:** since niggas is slacking on silcd/private ircd. I talked to my people @[redacted]nd they'd giving me an unlabeled box for priv8 ircd
(5:23:55 PM) **leondavidson@jabber.org/jabber.org:** btw you hear whats happening tonight?
(5:24:11 PM) **yohoho@jabber.ccc.de:** hmm?
(5:24:20 PM) **leondavidson@jabber.org/jabber.org:** cabin crew is getting killed
(5:24:50 PM) **leondavidson@jabber.org/jabber.org:** keep it between us
(5:25:05 PM) **leondavidson@jabber.org/jabber.org:** but jackals on a rampage. hes taking over their twitters and killing the crew
(5:25:11 PM) **leondavidson@jabber.org/jabber.org:** because of all the media whoring
(5:25:14 PM) **leondavidson@jabber.org/jabber.org:** and the drama
(5:25:17 PM) **yohoho@jabber.ccc.de:** that is awesome
(5:25:21 PM) **leondavidson@jabber.org/jabber.org:** ja
(5:25:25 PM) **yohoho@jabber.ccc.de:** fuck cabin
(5:25:26 PM) **yohoho@jabber.ccc.de:** fuck them hard
(5:25:34 PM) **yohoho@jabber.ccc.de:** especially[redacted] and[redacted]
(5:26:26 PM) **leondavidson@jabber.org/jabber.org:** I liked that they worked as a team (its no secret I like small teams, etc., and its effectiveness) but them niggas is all ego-tripping lamers.
(5:27:43 PM) **yohoho@jabber.ccc.de:** yes
(5:28:00 PM) **leondavidson@jabber.org/jabber.org:** let me know whats goodie with those [redacted]'s when you get a minute so I can move on to next shit
(5:28:04 PM) **leondavidson@jabber.org/jabber.org:** and whts good for friday?
(5:28:25 PM) **yohoho@jabber.ccc.de:** going to own a few .govs lol.
(5:28:34 PM) **yohoho@jabber.ccc.de:** just the [redacted]box
(5:28:58 PM) **leondavidson@jabber.org/jabber.org:** word up
(5:29:18 PM) **yohoho@jabber.ccc.de:** we need something every friday
(5:29:22 PM) **yohoho@jabber.ccc.de:** and plus
(5:29:26 PM) **yohoho@jabber.ccc.de:** since this one[redacted]box, probaly isnt' going to give us any additional leads
(5:29:29 PM) **yohoho@jabber.ccc.de:** and no mail
(5:29:32 PM) **yohoho@jabber.ccc.de:** may as well nuke that mofo
(5:29:35 PM) **yohoho@jabber.ccc.de:** all the mail is on[redacted]
(5:29:58 PM) **leondavidson@jabber.org/jabber.org:** jea
(5:41:54 PM) **leondavidson@jabber.org/jabber.org:**[redacted]=big target. they made a massive power move. they sent letters to 48 states (probably excluding alaska and hawaii) basically saying. give us 225million per prison and we'll manage all your prisoners
(5:42:49 PM) **leondavidson@jabber.org/jabber.org:** 10800000000 = 225*48 a year
(5:43:09 PM) **yohoho@jabber.ccc.de:** oh I know
(5:43:12 PM) **yohoho@jabber.ccc.de:** that is biggest target ever.
(5:43:16 PM) **yohoho@jabber.ccc.de:** they run plesk, in fact.
(5:43:18 PM) **yohoho@jabber.ccc.de:** but not vuln =(
(5:43:22 PM) **leondavidson@jabber.org/jabber.org:** fuck!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!1
(5:43:24 PM) **yohoho@jabber.ccc.de:** maybe I will search for other subdomains though
(5:43:26 PM) **yohoho@jabber.ccc.de:** did you ehar though?

(5:43:31 PM) **yohoho@jabber.ccc.de:** we have the 2nd largest private prisonc ompany
(5:43:34 PM) **yohoho@jabber.ccc.de:** right after [redacted]
(5:43:38 PM) **leondavidson@jabber.org/jabber.org:** no way
(5:43:41 PM) **leondavidson@jabber.org/jabber.org:** sweet
(5:43:45 PM) **yohoho@jabber.ccc.de:** yep. but there's not too uch on it =(
(5:43:48 PM) **yohoho@jabber.ccc.de:** it's on a bigass vhost
(5:43:54 PM) **yohoho@jabber.ccc.de:** windows target
(5:43:56 PM) **yohoho@jabber.ccc.de:** I put alex on it
(5:43:59 PM) **leondavidson@jabber.org/jabber.org:** sounds good
(5:44:09 PM) **yohoho@jabber.ccc.de:** we have bigger targets though
(5:44:15 PM) **yohoho@jabber.ccc.de:** jail management software developers
(5:44:29 PM) **yohoho@jabber.ccc.de:** my ultimate goal is to start adding funds on prisoner commisary accounts, changing outdates etc
(5:45:13 PM) **leondavidson@jabber.org/jabber.org:** I'm 100% on commisary
(5:45:34 PM) **leondavidson@jabber.org/jabber.org:** there's companies like jpay.com that allow you to send money to prisoners across the u.s. through their electronic system
(5:45:46 PM) **leondavidson@jabber.org/jabber.org:** even giving each prisoner a few dollars to eat changes their lives
(5:45:47 PM) **yohoho@jabber.ccc.de:** hmm interesting
(5:45:51 PM) **leondavidson@jabber.org/jabber.org:** and we'll send them a massive message
(5:45:54 PM) **leondavidson@jabber.org/jabber.org:** to all prisoners
(5:45:58 PM) **leondavidson@jabber.org/jabber.org:** that anonymous supports them
(5:45:59 PM) **leondavidson@jabber.org/jabber.org:** etc
(5:46:09 PM) **yohoho@jabber.ccc.de:** I agree that's what we need to do
(5:46:49 PM) **leondavidson@jabber.org/jabber.org:** you know how many prisoners are in there. no families. no loved ones. FUCKING BROKE. eating state pbj sandwiches that taste like shit because they simply have no way to buy any food or rollies to smoke
(5:46:53 PM) **leondavidson@jabber.org/jabber.org:** niggas gotta be in there suffering
(5:46:56 PM) **leondavidson@jabber.org/jabber.org:** its a fucking slave camp
(5:47:05 PM) **leondavidson@jabber.org/jabber.org:** having these prisoners work 14 hour shifts for 20 cents an hour
(5:47:25 PM) **yohoho@jabber.ccc.de:** yes it is ridiculous
(5:47:32 PM) **yohoho@jabber.ccc.de:** especially with immigrants
(5:47:46 PM) **yohoho@jabber.ccc.de:** they say they are illegal, but they lock them up and pay them welll below minimum wage
(5:47:57 PM) **yohoho@jabber.ccc.de:** in their prison sweatshops
(5:51:22 PM) **leondavidson@jabber.org/jabber.org:** http://www.theonion.com/articles/iran-worried-us-might-be-building-8500th-nuclear-w,27325/ tho meant as a joke is actually pretty sad state of reality
(6:46:52 PM) **leondavidson@jabber.org/jabber.org:** rofl
(6:46:58 PM) **leondavidson@jabber.org/jabber.org:** these niggas are wild
(6:47:00 PM) **leondavidson@jabber.org/jabber.org:** [redacted]
(6:47:13 PM) **leondavidson@jabber.org/jabber.org:** using dns amplification attacks to shut down the root dns servers
(6:48:40 PM) **yohoho@jabber.ccc.de:** yes if oyu hit root dns servers shit will go wild
(6:48:45 PM) **yohoho@jabber.ccc.de:** maybe more people will use services like opendns

(6:53:21 PM) **yohoho@jabber.ccc.de:** ok
(6:53:25 PM) **yohoho@jabber.ccc.de:** going to hit those [redacted] for oyu now
(6:53:35 PM) **leondavidson@jabber.org/jabber.org:** kk
(6:59:41 PM) **leondavidson@jabber.org/jabber.org:** http://exploitshop.wordpress.com/2012/02/15/ms12-013-vulnerability-in-c-run-time-library-could-allow-remote-code-execution/
(7:01:40 PM) **yohoho@jabber.ccc.de:** yo I just owned another major target
(7:01:40 PM) **yohoho@jabber.ccc.de:** dumping via sqlmap now
(7:01:40 PM) **yohoho@jabber.ccc.de:** this will be delicious
(7:01:57 PM) **leondavidson@jabber.org/jabber.org:** aRF
(7:02:07 PM) **leondavidson@jabber.org/jabber.org:** prison shiz??
(7:03:34 PM) **yohoho@jabber.ccc.de:** nah
(7:03:34 PM) **yohoho@jabber.ccc.de:** well
(7:03:39 PM) **yohoho@jabber.ccc.de:** I already have a lot of prison shit lined up
(7:03:41 PM) **yohoho@jabber.ccc.de:** need help actually
(7:03:47 PM) **yohoho@jabber.ccc.de:** [redacted] = rooted
(7:03:52 PM) **yohoho@jabber.ccc.de:** I uploadd mails to our .onion
(7:03:56 PM) **yohoho@jabber.ccc.de:** elche has been gong through it
(7:05:11 PM) **leondavidson@jabber.org/jabber.org:** faggot ass tor and my vpn dont like each other but good shit looking it over
(7:05:55 PM) **leondavidson@jabber.org/jabber.org:** prison systems software?
(7:06:12 PM) **yohoho@jabber.ccc.de:** yes
(7:06:16 PM) **yohoho@jabber.ccc.de:** the mail contains lots of info
(7:06:27 PM) **yohoho@jabber.ccc.de:** I just dont ahve time to follow up on it
(7:06:30 PM) **yohoho@jabber.ccc.de:** which is why we need help
(7:06:31 PM) **leondavidson@jabber.org/jabber.org:** plz tell me we have access to soutrce codes
(7:06:44 PM) **yohoho@jabber.ccc.de:** I barely looked through it
(7:06:52 PM) **yohoho@jabber.ccc.de:** we need you to get your hands dirty
(7:09:09 PM) **leondavidson@jabber.org/jabber.org:** so get me datas nigga
(7:09:20 PM) **leondavidson@jabber.org/jabber.org:** faggot tor i cant ever access
(7:10:36 PM) **yohoho@jabber.ccc.de:** https[redacted]
(7:10:43 PM) **yohoho@jabber.ccc.de:** and I already dumped mail and rendered it
(7:10:44 PM) **yohoho@jabber.ccc.de:** 1 min
(7:11:11 PM) **leondavidson@jabber.org/jabber.org:** kk
(7:27:03 PM) **yohoho@jabber.ccc.de:** https:/[redacted] and www[redacted]
(7:27:05 PM) **yohoho@jabber.ccc.de:** those are all rooted
(7:27:10 PM) **yohoho@jabber.ccc.de:** none of the others worked
(7:27:29 PM) **yohoho@jabber.ccc.de:** now on [redacted] is not on there, but there is ctrl.php3, which accepts a POST parameter of x to run commands
(7:27:39 PM) **yohoho@jabber.ccc.de:** the other two both have core.php
(7:27:57 PM) **yohoho@jabber.ccc.de:** they all look like they have hundreds of domains and mails
(7:28:01 PM) **yohoho@jabber.ccc.de:** hopefully they wil put it to good use
(7:28:08 PM) **yohoho@jabber.ccc.de:** and hopefulyl were getitngs omething out of all this
(7:29:04 PM) **leondavidson@jabber.org/jabber.org:** trust me negro everything i do serves a purpose ;P

(7:43:48 PM) **yohoho@jabber.ccc.de:** shadow_dxs
(7:43:53 PM) **yohoho@jabber.ccc.de:** he is known snitch right?
(7:44:27 PM) **leondavidson@jabber.org/jabber.org:** not really hes a troll mainly. likes to fuck with people from both sides
(7:44:31 PM) **leondavidson@jabber.org/jabber.org:** old carder
(7:44:39 PM) **leondavidson@jabber.org/jabber.org:** font fixed
(7:44:52 PM) **yohoho@jabber.ccc.de:** lol
(7:45:10 PM) **yohoho@jabber.ccc.de:** check priv8haha for [redacted] mails
(7:45:14 PM) **yohoho@jabber.ccc.de:** needs work
(7:45:16 PM) **leondavidson@jabber.org/jabber.org:** trolls anons and prosec ppl. e.g. he recently doxed awinees girlfriend and posted her pics
(7:45:19 PM) **leondavidson@jabber.org/jabber.org:** kk looking
(7:45:32 PM) **yohoho@jabber.ccc.de:** he wasn't br1cksqu4d ?
(7:45:42 PM) **yohoho@jabber.ccc.de:** and why have I heard nothing but rumors about him being a snitch
(7:46:37 PM) **leondavidson@jabber.org/jabber.org:** no he wasnt and youve probably heard it because he hangs with prosec ppl
(7:47:01 PM) **leondavidson@jabber.org/jabber.org:** 2600 and now reapersec etc
(7:47:32 PM) **leondavidson@jabber.org/jabber.org:** i get good laughs from him watching him troll his own ppl
(7:53:25 PM) **yohoho@jabber.ccc.de:** ok yo
(7:53:28 PM) **yohoho@jabber.ccc.de:** got shell on this high profile target
(7:53:29 PM) **yohoho@jabber.ccc.de:** LULZ
(7:54:28 PM) **leondavidson@jabber.org/jabber.org:** ARF
(7:54:32 PM) **leondavidson@jabber.org/jabber.org:** good shit
(7:55:24 PM) **leondavidson@jabber.org/jabber.org:** goin through [redacted] mails
(7:55:31 PM) **yohoho@jabber.ccc.de:** billing is the major one
(7:55:32 PM) **yohoho@jabber.ccc.de:** and also talk to elche
(7:55:35 PM) **yohoho@jabber.ccc.de:** because he already looked through em
(7:55:43 PM) **yohoho@jabber.ccc.de:** basically you can see references to 'ftp conneciton' etc
(7:57:40 PM) **leondavidson@jabber.org/jabber.org:** kk
(8:11:23 PM) **yohoho@jabber.ccc.de:** Yo I think this i smajor target.
(8:11:27 PM) **yohoho@jabber.ccc.de:** Our engineers worked closely with one of the UK's largest police forces to help develop what is undoubtedly one of the most sophisticated Command and Control systems in the world.

(8:11:43 PM) **leondavidson@jabber.org/jabber.org:** o wow
(8:11:47 PM) **leondavidson@jabber.org/jabber.org:** thats nice
(8:11:50 PM) **leondavidson@jabber.org/jabber.org:** got mails?
(8:11:52 PM) **yohoho@jabber.ccc.de:** and that's not all either
(8:11:55 PM) **yohoho@jabber.ccc.de:** yes I think so
(8:11:58 PM) **yohoho@jabber.ccc.de:** at least some mail
(8:12:05 PM) **yohoho@jabber.ccc.de:** not sure if it is the main mail server for the entire company
(8:12:58 PM) **leondavidson@jabber.org/jabber.org:** mhm
(8:15:14 PM) **yohoho@jabber.ccc.de:** and
(8:15:17 PM) **yohoho@jabber.ccc.de:** this guy just owned [redacted]

(8:15:18 PM) **leondavidson@jabber.org/jabber.org:** hows user db? full of uk feds?
(8:15:29 PM) **yohoho@jabber.ccc.de:** unfortunately the DB I have so far isn't much
(8:15:34 PM) **yohoho@jabber.ccc.de:** just the admin logins to this one site
(8:15:41 PM) **yohoho@jabber.ccc.de:** barely begun digging into the box
(8:15:46 PM) **yohoho@jabber.ccc.de:** fuck homey
(8:15:52 PM) **yohoho@jabber.ccc.de:** not to mention we gotta wrap up this [redacted] box
(8:15:53 PM) **yohoho@jabber.ccc.de:** and
(8:15:58 PM) **yohoho@jabber.ccc.de:** helping this guy get on [redacted]
(8:16:03 PM) **leondavidson@jabber.org/jabber.org:** the guy who owned [redacted] i that just kid?
(8:16:05 PM) **yohoho@jabber.ccc.de:** it's too much
(8:16:09 PM) **yohoho@jabber.ccc.de:** canc3r
(8:16:13 PM) **yohoho@jabber.ccc.de:** just hit me up too thogh
(8:16:24 PM) **yohoho@jabber.ccc.de:** not sure if he is legit he says sql injection
(8:16:28 PM) **yohoho@jabber.ccc.de:** bout a european gov site
(8:16:45 PM) **leondavidson@jabber.org/jabber.org:** hes been telling me shit but i thought he was fed
(8:16:52 PM) **leondavidson@jabber.org/jabber.org:** cause he namedropped me
(8:16:54 PM) **yohoho@jabber.ccc.de:** yeah I got suspicious too
(8:16:55 PM) **yohoho@jabber.ccc.de:** about just
(8:17:09 PM) **yohoho@jabber.ccc.de:** he started asking what team I was, and how many ppl were in atnisec, and whether we got that FBI phonecall
(8:17:10 PM) **yohoho@jabber.ccc.de:** lol.
(8:26:54 PM) **leondavidson@jabber.org/jabber.org:** yeh. fed to me honestly

#antisecredhack.log

--- Log opened Wed Jan 25 21:54:12 2012
21:54 -!- Sabu [sabu@security.anonymo.us] has joined #antisecRedHack
21:54 -!- Irssi: #antisecRedHack: Total of 1 nicks [1 ops, 0 halfops, 0 voices, 0 normal]
21:54 -!- Irssi: Join to #antisecRedHack was synced in 2 secs
21:54 -!- mode/#antisecRedHack [+s] by Sabu
22:03 !sabit.cryto.net Sabu invited RedStar into the channel.
22:03 !kerpia.cryto.net Sabu invited sup_g into the channel.
22:05 -!- sup_g [ghost@51BC5033.870C7BE1.49E80F3.IP] has joined #antisecRedHack
22:05 -!- RedStar [cHiEf@B0266B94.7F13FC28.9AEC544A.IP] has joined #antisecRedHack
22:05 < RedStar> re my brothers
22:05 <@Sabu> hey :)
22:05 < RedStar> .]
22:05 <@Sabu> RedStar: meet my brother sup_g
22:05 <@Sabu> sup_g: meet my good friend RedStar
22:05 < sup_g> sup redstar, big fan
22:05 < sup_g> as an anarchist communist
22:06 < sup_g> owning some shit for you =)
22:06 < RedStar> sup hello my brother, nice t m u ;)
22:06 <@Sabu> its been a long time man. I was worried about you. I read lots of arrests in [redacted]:|
22:06 <@Sabu> your team ok?
22:06 < RedStar> super i found one bug police of state [redacted]
22:06 < RedStar> [redacted]
22:07 < sup_g> [redacted]
22:07 < sup_g> ^ rooted for you
22:07 < sup_g> more coming
22:07 <@Sabu> ;)
22:07 <@Sabu> sup_g: I got more [redacted] targets as well. I'll send you shortly
22:08 < sup_g> k
22:08 <@Sabu> redstar: we rooted these for you - have your team get into the boxes and do what you do ;)
22:08 < RedStar> super sup, thanks thank on behalf of my people my brothe
22:08 < sup_g> redstar how do you want these? webshell with a suidshell backdoor?
22:08 < sup_g> [redacted]
22:08 < sup_g> is that enough for yall?
22:09 < RedStar> no sql injection
22:09 <@Sabu> no its already shelled for you and rooted
22:09 < RedStar> its very important[redacted]but i an found "admin panel"
22:09 < RedStar> i found user pass
22:10 < RedStar> aha
22:10 < RedStar> i understand. but how many sites is server?
22:10 < sup_g> haven't even looked
22:10 < sup_g> sorry I will be busy for about 25 minutes, you will still be here?
22:11 < RedStar> yes yes
22:11 < RedStar> Make yourself at home
22:11 < RedStar> i am very bad english sory ;)
22:12 < sup_g> that's ok =)
22:12 < RedStar> google rulez ;)
22:12 < sup_g> we are on the same team
22:12 < RedStar> ok i waiting
22:13 <@Sabu> ;)
22:13 <@Sabu> RedStar: is your team OK? I read a lot of arrests in [redacted] I was worried for you
22:14 < RedStar> ok Sabu, I am glad, only give me the time of the week until the end of preparation, a nice server rootlamak, ok?
22:15 < RedStar> yes sabu
22:15 <@Sabu> yes take your time
22:15 < RedStar>[redacted]is nig prison
22:15 < RedStar> big..
22:16 < RedStar> evreday arests dissident
22:16 <@Sabu> not good.. hopefully with these [redacted]roots you can make big impact
22:16 < sup_g> there's a lot
22:16 < sup_g> however
22:16 < RedStar> We stopped because of a little away from him. benefits, but do

#antisecredhack.log

not fear death;)
22:16 < sup_g> you need to make sure you dump email and mysql databases
22:17 <@Sabu> if I am not around /msg sup_g he is my trusted friend. you can communicate with him directly and he is fellow anarchist :)
22:17 < sup_g> and mirror them online
22:17 < sup_g> so you can embarass them most
22:17 < sup_g>)
22:17 < sup_g> ;)
22:17 < RedStar> [redacted]
22:18 < sup_g> do you all have some mirroring server that you can host the stolen mail spools and databases?
22:18 < RedStar> sup_g brother Look at You. We could not find admin panel. This point is very important
22:18 < sup_g> have you ran that vulnerability through sqlmap or hajiv?
22:19 < RedStar> yes
22:19 < RedStar> Website : [redacted]
22:19 < RedStar> Database [redacted]
22:19 < RedStar> Table : members
22:19 < RedStar> [redacted]
22:19 < RedStar> [redacted]
22:19 < RedStar> [redacted]
22:19 < RedStar> [redacted]
22:19 < RedStar> [redacted]
22:19 < RedStar> [redacted]
22:19 < RedStar> [redacted]
22:19 < RedStar> yes hajiv its runned this server
22:20 < sup_g> nice have you tried cracking those hashes and checking against their email accounts?
22:20 < sup_g> lol @gmail
22:21 < RedStar> i am download all information scree
22:21 < RedStar> +t
22:21 < sup_g> sorry I am still sort of busy for ~25 minutes =(but still here
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:21 < RedStar> [redacted]
22:23 < RedStar> Website : [redacted]
22:23 < RedStar> Database : [redacted]
22:23 < RedStar> Table : [redacted]
22:23 < RedStar> username:password:
22:23 < RedStar> [redacted]
22:24 <@Sabu> nice let me see if I can find admin

#antisecredhack.log

22:28 < RedStar> i am found all screet information but i am not founded admin cp ;)
22:29 < RedStar> frustrating. if you can not get, let's public information?
22:30 < RedStar> Sabu brother look this [redacted]
22:30 <@Sabu> RedStar: no public information :) save it until we find admin panel
22:30 <@Sabu> ok
22:32 < RedStar> ok ;)
22:35 <@Sabu> RedStar: stay here ok ? I'll be back in a few minutes
22:35 < sup_g> back
22:36 < sup_g> yes redstar you should hold onto that until we can find osmething to do with those passwords
22:36 < sup_g> maybe if you login to their emails it will contain FTP info to that domain
22:37 < sup_g> ok rooting more of these targets for you
22:39 < RedStar> super brother, this irc server is now always open in the meantime?
22:40 < sup_g> [redacted]
22:40 < sup_g> LOL.
22:40 < sup_g> yes.
22:40 < RedStar> vauv ;)
22:41 < RedStar> 700 super, how many gov ?
22:41 < sup_g> 1 min.
22:42 < sup_g> another box, 83
22:42 < sup_g> [redacted]
22:42 < RedStar> I like defacer ;))
22:42 < sup_g> you need to make sure you dump the mail
22:42 < sup_g> that is important
22:42 < sup_g> it is all in [redacted] on these boxes
22:43 < RedStar> qmail ;)
22:44 < RedStar> you make reverse?
22:44 < RedStar> comparison named.conf etc?
22:44 < sup_g> I can send you a reverse shell
22:44 < RedStar> ah oky
22:45 < RedStar> you rooting kernel or this server safe mode off?
22:49 < sup_g> [redacted]
22:49 < sup_g> [redacted]
22:49 < sup_g> LOLOL
22:49 < RedStar> no ;)) [redacted] lol :P
22:50 < sup_g> they may not all be .govs
22:50 < sup_g> obviously
22:50 < RedStar> yes does not matter, I think goes to talk instead of ;)
22:51 < sup_g> ok
22:51 < sup_g> [redacted] rooted
22:51 < sup_g> [redacted] rooted
22:51 < sup_g> [redacted] rooted
22:51 < sup_g> [redacted] rooted
22:51 < sup_g> which do you want first?
22:52 < sup_g> also [redacted]
22:52 < sup_g> [redacted]
22:52 < sup_g> [redacted]
22:52 < sup_g> [redacted]
22:52 < sup_g> but they are windows
22:52 < sup_g> I can get you ftp passwords for all accounts tho
22:57 < sup_g> u there?
22:57 < RedStar> oh ftp account super
22:57 < RedStar> i am here i find admin panel
22:58 < sup_g> on that police one?
22:58 < sup_g> upload backdoor.asp =)
22:58 < RedStar> yes
22:58 < sup_g> err .php
22:58 < RedStar> You see a break, [redacted]
22:58 < sup_g> [redacted]
22:58 < RedStar [redacted]
23:18 <@Sabu> sup_g: nice :) mad domains on those boxes
23:19 < RedStar> big job brothers
23:19 < sup_g> yeah it's pretty crazy
23:20 < RedStar> When the index to throw, and what to write?
23:23 < RedStar> There are many denunciation mail;) [redacted]

#antisecredhack.log

[redacted]
23:24 < sup_g> you can download via thunderbird over tor
23:24 < sup_g> then render with mhonarc
23:24 < sup_g> do you ahve a server that you can store/mirror/deploy their mail ?
23:28 < RedStar> yes this mail police of [redacted] denunciation mail. cache information
23:34 < sup_g> omfg, so much mail
23:34 < sup_g> ls -al | [redacted] wc
23:34 < sup_g> 616 5544 43813
23:34 < sup_g> 616 [redacted]domains have mail stored here
23:35 < sup_g> redstar do you have a bounce box that you can safely wget large amounts of mail from?
23:37 < RedStar> bounce box?
23:38 < sup_g> hacked server
23:38 < sup_g> someplace you can safely wget [redacted]
23:40 < RedStar> ah no, i make sql injection after system getting mail passwd
23:40 < RedStar> [redacted]
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:40 < RedStar>
23:41 < RedStar>
23:41 < RedStar>
23:41

#antisecredhack.log

23:41 < RedStar> [redacted]
23:41 < RedStar> [redacted]
23:41 < RedStar> [redacted]
23:41 < RedStar> [redacted]
23:41 < RedStar> [redacted]
23:41 < RedStar> [redacted]
23:43 < RedStar> [redacted]
cef:
23:49 < sup_g> that's good
23:49 < sup_g> I am working on these other [redacted] tho
23:52 < RedStar> okay sup i am here comrade
23:55 < sup_g> ok I will have a shell for you very soon
23:55 < RedStar> ok brother ;)
23:58 < sup_g> [redacted]
23:58 < sup_g> then do this:
23:58 < sup_g> [redacted]
23:59 < sup_g> ;) ;)
--- Day changed Thu Jan 26 2012
00:00 < sup_g> there are DOZENS of mail for [redacted]
00:03 < sup_g> you got it?
00:05 < RedStar> yeps
00:05 < RedStar> [redacted]
00:05 < RedStar> [redacted]
00:05 < RedStar> [redacted]
00:05 < RedStar> [redacted]
00:05 < RedStar> [redacted]
00:05 < RedStar> [redacted]
00:05 < sup_g> also
00:05 < sup_g> make sure you wipe that shit when we rm
00:06 < sup_g> but first priority is getting mail
00:06 < sup_g> [redacted]
00:06 < sup_g> damn that's a lot of mail.
00:07 < RedStar> 26[redacted] super
00:07 < sup_g> i'll copy it
00:07 < RedStar> nice job comrade
00:07 < RedStar> okay.
00:08 < sup_g> I am making "all" mail and "justgov" mail
00:08 < sup_g> cause "all" will probably be > 100GB or some crazy shit
00:09 < RedStar> 100 gb :) user in [redacted] is download 4 days :)
00:13 < sup_g> [redacted]
  <- 550MB
00:13 < sup_g> downloading and verifying
00:14 < RedStar> my internet very very fast or i am downloading its file min 1 day ;(shitnet..
00:14 < sup_g> you using proxy?
00:14 < sup_g> (I can wipe logs though)
00:15 < sup_g> ok that [redacted] is good
00:15 < sup_g> real good =)
00:19 < RedStar> yes and my ISP is shit ;(
00:19 < RedStar> you download?
00:19 < RedStar> i say my comrade, is redhack member, he is download..
00:19 < sup_g> ok
00:20 < sup_g> are you all able to upload that mail somewhere?
00:20 < sup_g> and release it as torrent
00:20 < sup_g> and yes I did download and verify
00:21 < RedStar> ok
00:21 < RedStar> and bad news [redacted]
00:22 < RedStar> [redacted]
00:22 < sup_g> it was owned already?
00:22 < sup_g> lol,
00:23 < sup_g> well now you have the mail
00:23 < sup_g> that might have the dirt, the controversy, the secrets
00:24 < RedStar> ok
00:28 < RedStar> he is download its time

#antisecredhack.log

00:30 < sup_g> did that box go down?
00:30 < sup_g> 94 = dead?
00:32 < sup_g> [redacted]
00:32 < sup_g> drwxr-xr-x 13 root root [redacted] Dec 16 12:08 [redacted]
00:32 < sup_g> drwxr-xr-x 14 root root [redacted] Dec 16 12:08 [redacted]
00:32 < sup_g> drwxr-xr-x 13 root root [redacted] Dec 16 12:08 [redacted]
00:32 < sup_g> drwxr-xr-x 13 root root [redacted] Dec 16 12:08 [redacted]
00:32 < sup_g> drwxr-xr-x 13 root root [redacted] Dec 16 12:08 [redacted]
00:32 < sup_g> drwxr-xr-x 13 root root [redacted] Dec 16 12:08 [redacted]
00:32 < sup_g> drwxr-xr-x 13 root root [redacted] Dec 16 12:08 [redacted]
00:33 < RedStar> nice its time how mny domain plus?
00:33 < sup_g> hundreds again
00:33 < RedStar> :)
00:34 < RedStar> man is real worker ;)
00:35 < sup_g> working class =)
00:36 <@Sabu> ;)
00:37 < sup_g> ok homey
00:37 < sup_g> https:[redacted]
00:38 < sup_g> [redacted]
00:38 < sup_g> [redacted] <- is the cleartext plesk password
00:38 < sup_g> [redacted]
00:39 < RedStar> [redacted] admin is very idiot ha? ;))
00:40 < sup_g> lol.
00:40 < RedStar> i connect
00:40 < sup_g> drwxr-x---   9 root   popuser [redacted] Apr 13 2011 [redacted]
00:40 < sup_g> drwxr-x--- 20 root   popuser [redacted] Nov 14 11:26 [redacted]
00:40 < sup_g> drwx------ 12 popuser popuser [redacted] Dec 16 12:13 [redacted]
00:40 < sup_g> drwxr-x---   2 root   popuser [redacted] Mar 30 2011 [redacted]
00:40 < sup_g> drwx------   3 popuser popuser [redacted] Dec 16 12:13 [redacted]
00:40 < sup_g> drwxr-x---   2 root   popuser [redacted] Mar 30 2011 [redacted]
00:40 < sup_g> drwxr-x---   2 root   popuser [redacted] Mar 30 2011 [redacted]
00:40 < sup_g> drwxr-x---   6 root   popuser [redacted] Mar 30 2011 [redacted]
00:40 < sup_g> drwxr-x---   2 root   popuser [redacted] Apr 25 2011 [redacted]
00:41 < sup_g> drwx------   3 popuser popuser [redacted] Dec 16 12:13 [redacted]
00:41 < sup_g> ~ 40 government mail spools =)
00:41 < RedStar> 654 total
00:41 < RedStar> :)
00:41 < sup_g> they will FREAK
00:42 < sup_g> -rw-r--r-- 1 root   root   141032724 Jan 25 19:52 [redacted] only 140MB =(
00:42 < sup_g> still something though
00:43 <@Sabu> a lot of great targets
00:44 < RedStar> Sabu brother, where did you get this defacer, man of genius:))
00:45 <@Sabu> he is my very good friend :) you might have to borrow him for your team haha
00:45 < RedStar> ;)))
00:45 < sup_g> <- dirty red =)
00:45 < sup_g> black and red
00:45 < RedStar> plus he is anachist communist ;) perfect man ;)
00:45 <@Sabu> ;D
00:47 < sup_g> hopefully the mail will have a lot of dirty secrets on the government
00:47 < sup_g> also before you deface
00:47 < RedStar> Sabu; is generated young fans
http://www.youtube.com/watch?v=705eX5zUOm4
00:47 < sup_g> make sure you shred
00:47 < sup_g> [redacted]

#antisecredhack log

00:48 < sup_g> and also [redacted]
00:48 < sup_g> shred
00:49 < sup_g> also see alldatabases.sql
00:49 < sup_g> download that shit =)
00:49 <@Sabu> very nice intro. you should throw our group name in it.. #antisec
:)
00:49 <@Sabu> is that for the defacements?
00:49 < RedStar> Sup: [redacted]
00:50 < sup_g> lol.
00:50 < sup_g> [redacted]
00:50 < sup_g> hah just kidding
00:52 < RedStar> yes and one supris, we make one group is name "Others".. For the
ddos and real miting.. its time many people get to know
00:52 < RedStar> real protest and meeting
00:53 < sup_g> another
00:53 < sup_g> ls -al /var/www/vhosts | [redacted]
00:53 < sup_g> drwxr-xr-x 15 root root [redacted] Jun 16 2011 [redacted]
00:53 < sup_g> drwxr-xr-x 14 root root [redacted] Sep 9 2010 [redacted]
00:53 < sup_g> drwxr-xr-x 14 root root [redacted] Sep 9 2010 [redacted]
00:54 < sup_g> drwxr-xr-x 14 root root [redacted] Sep 9 2010 [redacted]
00:54 < sup_g> drwxr-xr-x 13 root root [redacted] Feb 27 2010 [redacted]
00:54 < sup_g> drwxr-xr-x 13 root root [redacted] Feb 27 2010 [redacted]
00:54 < sup_g> drwxr-xr-x 14 root root [redacted] Jun 25 2010 [redacted]
00:54 < sup_g> good?
00:54 < sup_g> ls -al /var/qmail/mailnames | [redacted]
00:54 < sup_g> drwx------   6 popuser popuser [redacted] Jun 23 2011 [redacted]
00:54 < sup_g> drwx------ 12 popuser popuser [redacted] Sep 9 2010 [redacted]
00:54 < sup_g> drwx------   2 popuser popuser [redacted] Sep 9 2010 [redacted]
00:54 < sup_g> drwx------   2 popuser popuser [redacted] Sep 9 2010 [redacted]
00:54 < sup_g> drwx------   3 popuser popuser [redacted] Sep 9 2010 [redacted]
00:54 < sup_g> drwx------   3 popuser popuser [redacted] May 14 2010 [redacted]
00:54 < sup_g> drwx------ 11 popuser popuser [redacted] Jan 16 16:04 [redacted]
00:54 < sup_g> drwx------   2 popuser popuser [redacted] Jun 25 2010 [redacted]
00:54 < sup_g> moar mail
00:55 < RedStar> r u make zip? download link?
01:00 < sup_g> [redacted]
01:01 < RedStar> hahha [redacted]
01:01 < RedStar> [redacted]
01:04 < sup_g> lol.
01:04 < sup_g> getting more now
01:04 < RedStar> :)
01:04 < sup_g> already dumped their mail; do ls -al
01:07 < sup_g> drwxr-xr-x 14 root root [redacted] Feb 8 2009 [redacted]
01:07 < sup_g> drwxr-xr-x 14 root root [redacted] Mar 22 2010 [redacted]
01:07 < sup_g> drwxr-xr-x 14 root root [redacted] Feb 8 2009 [redacted]
01:07 < sup_g> good ones?
01:08 < RedStar> [redacted]
01:08 < RedStar> 345 domain and one sites fascist party [redacted] ;)
01:09 < sup_g> which one was that?
01:09 < sup_g> did we get that one yet?
01:09 < RedStar> bad is not open ;([redacted]
01:09 < RedStar> national party of [redacted]
01:10 < RedStar> one a branch
01:13 < sup_g> [redacted] <- no mail though =(
01:16 < RedStar> [redacted] ;) national party :) [redacted]
01:17 < sup_g> rooted ;)
01:17 < RedStar> :)
01:17 <@Sabu> good work ;)
01:18 <@Sabu> you gentlemen realize this massive hack is going to make news in
europe [redacted]

#antisecredhack.log

01:18 <@Sabu> :X
01:19 < sup_g> take your time redstar
01:19 < sup_g> look at all their domains, all their files, databases, mail
01:19 < sup_g> get it all up online for other people to read
01:19 <@Sabu> yeah
01:19 < sup_g> then deface / rm
01:19 < RedStar> needs is a good text for the index
01:21 < sup_g> that's all I have for now
01:22 < sup_g> next time we will have some windows boxes for you
01:22 < RedStar> sup brother when do we? other people need? you prepare the index?
01:22 < sup_g> you don't want to read their mail first?
01:22 <@Sabu> RedStar: look through the servers, find important mails
01:23 <@Sabu> you might find corruption evidence
01:23 < sup_g> redstar when we own something we take time and find everything first
01:23 < sup_g> I don't have time to look through all their files and mail? thats your job =)
01:23 < RedStar> ok i say my comrade is look your mail zip
01:25 <@Sabu> while you guys read mails, you have time to prepare nice defacement. message. etc
01:26 < RedStar> But I do not think anything will come to the emails, because these sites usually in small towns, villages, towns sites
01:27 < sup_g> it still adds insult to injury =)
01:27 < sup_g> throw gasoline on the flames
01:28 < RedStar> its not importand sites.. for example http:[redacted] is towns sites..
01:28 <@Sabu> yeah
01:29 <@Sabu> well my brother we leave it in your hands :) just tweet us when you do the hack to @anonymousIRC and @anonymouSabu so we can spread your message
01:29 <@Sabu> I'll look for more [redacted]targets
01:29 <@Sabu> better yet you find big [redacted] targets let us know we'll try loookin at them
01:29 < RedStar> ok brother [redacted] user:[redacted] pass[redacted]
01:32 < RedStar> for example[redacted]
-> is police capital of[redacted] subjet "155" screet mail notice
01:34 <@Sabu> mhm
01:34 < RedStar> for example one found admin panel after we make index, is big job for [redacted]i finder user and pass but i am not find admin panel i am crazy 2 days i am not found ;(
01:36 < RedStar>
http:[redacted]
01:36 < RedStar> sql helper sup
01:37 < RedStar> one hacked this server is big job.. and[redacted]sql bug
01:37 < RedStar> sqli helper 2.7
[redacted]
01:39 < RedStar> shit! .. went to a power I hope that as soon as the battery
01:39 < RedStar> sup deface incident when we do? tomorrow? weekend?
01:40 < sup_g> weekend Im thinking
01:40 < sup_g> take your time
01:40 < sup_g> we have to at LEAST upload all the mail
01:41 <@Sabu> weekend is good
01:41 < RedStar> ok
01:42 < RedStar> Saturday 20:00 this place, good?
01:43 <@Sabu> ja meet us here
01:43 <@Sabu> we'll organizee
01:43 < RedStar> because Now in the morning 03:53 ;)
01:44 <@Sabu> ;) ok my brother good to see you
01:44 < RedStar> friday or saturday 20 or 21 or 22 is good.. ?
01:44 <@Sabu> get rest ok?
01:45 < RedStar> ok sabu, sup okey? and Do I need him for the index?
01:46 < RedStar> extra man..
01:47 < RedStar> you need an extra man in there? i speaking shit english sory ;)
01:47 <@Sabu> haha
01:47 <@Sabu> the index you can do make it nice ;)
01:48 <@Sabu> we talk soon ok brother? going to sleep